Patelco
CREDIT UNION

Online Safety Tips

Safer Online Banking

TIP: Type patelco.org directly into the address bar, or bookmark it and use the bookmark.

Why: This will ensure that you reach the credit union's real website, not a fake copy. If you search for a financial institution's name to find their website, it's possible you'll end up on a fake site set up by fraudsters.

TIP: Use a strong password that you do not use anywhere else and change it regularly.

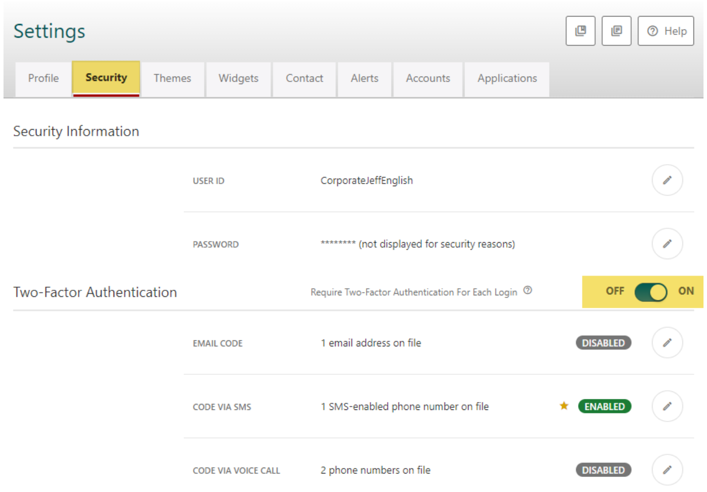
Why: This protects your account if your password from another site becomes exposed.

Your password should be at least 8 characters long (14 or more is better) and should contain a mixture of letters, numbers, and symbols. Do not use any part of your name, User ID or username, or information such as your Social Security Number, phone number, credit card number, or birthdate.

TIP: Set up two-factor authentication.

Why: Even if someone gets your password, they cannot access your account without verification code sent to you.

How: Log in to online banking, go to **Settings** and then **Security**. Tap or click the Two-Factor Authentication toggle to **ON**. You can also select how to receive the code. Most people find that getting the verification code by text message is fast and easy.



Settings

Security Information

USER ID CorporateJeffEnglish

PASSWORD ******** (not displayed for security reasons)

Two-Factor Authentication Require Two-Factor Authentication For Each Login OFF ON

EMAIL CODE 1 email address on file DISABLED

CODE VIA SMS 1 SMS-enabled phone number on file ★ ENABLED

CODE VIA VOICE CALL 2 phone numbers on file DISABLED

TIP: Avoid using public wifi networks or shared computers for credit union and banking.

Why: Using public networks can allow someone to “eavesdrop” on your activity. A shared computer could contain malware or could allow the person using it after you to access your account.

TIP: Set up alerts for your credit union account.

Why: Patelco can notify you if someone accesses your online banking account, changes your personal information, or performs certain types of financial transactions.

How: Log in to online banking, and go to **Settings**, then select **Security** and then **Authentication**. Tap or click the Online Banking Access Alert toggle to **ON** and select one or more ways to get the alert notification.

TIP: Protect your personal devices with a password, fingerprint, or facial recognition.

Why: This makes it harder for a thief to get into your phone.

TIP: Use your phone’s fingerprint or facial recognition security for your online banking login.

How: Install the Patelco Mobile App on your phone and, when prompted, allow the app to use your phone’s fingerprint or facial recognition feature.

Why: Your login experience will be fast and secure.

TIP: Save your online banking password in a vault, not in a web browser.

Why: If someone uses your computer or mobile device after you, they could gain access to your personal accounts. A vault that requires you to enter a password, use your fingerprint and/or password so that the website can access passwords is much safer.

TIP: Log out and close the tab when you finish your banking.

Why: If anyone uses your computer after you, they could access your account. Closing the tab helps to ensure that no details are temporarily cached.

TIP: Don’t be fooled by caller ID – verify if you’re ever suspicious.

Why: Fraudsters may spoof caller ID to make it appear as though a call is coming from Patelco. Remember, we’ll never call you and ask for sensitive information. If you ever get a funny feeling about a call (or text) you receive, ignore it and contact us directly by visiting a branch or calling **800.358.8228**.

TIP: Don't provide personal or account information unless you initiate contact, and never via email.

Why: Patelco will never call, email, or text you to request this type of information. Hackers and identity thieves try to trick people into revealing personal information. If you receive a call, text, or email asking you to give your personal or account information, contact Patelco directly using the contact information on this card. Don’t use any contact information provided in the suspicious call or message.

TIP: Check your account regularly for unauthorized charges or withdrawals; check your statements monthly.

Why: This will help you catch any unauthorized activity that may not have been identified through alerts or your routine logins.

How: Use eStatements instead of paper statements that can be lost or stolen. Put it on your calendar monthly to log in and review your transactions. You can also view your latest transactions in online banking at any time – just head to **patelco.org/onlinelogin**.

Additional Digital Safety Tips

TIP: Keep your computer, phone, and software up to date with security patches.

Why: This will help to protect you from common security attacks.

TIP: Use antivirus and antispyware applications.

Why: These types of software help to block some of the attacks on the Internet.

TIP: Make sure websites are secure and authentic (look for https – the “s” stands for “secure”).

Why: HTTPS means that communication between you and the website’s server is encrypted (protected from unauthorized reading).

TIP: Beware of email attachments and of free software from unknown sources.

Why: These can contain malware that could compromise your device or personal information. An insecure or malicious banking application could lead to a criminal accessing your money or stealing your identity.

TIP: Understand the privacy policy for apps you download or services you use.

Why: Applications could access or share your personal data.

TIP: Never save your debit card number on a website.

Why: If the website gets compromised, criminals will have direct access to your bank account.

How: If you’re using a debit card and a website asks if you want to save it, always say no.

TIP: Report lost or stolen cards right away

Why: This limits your liability, and the credit union can lock your accounts to protect you.

How: Call Patelco at **800.358.8228** if one of your cards is ever lost or stolen.

TIP: Check your annual credit report at least once a year for unauthorized accounts opened in your name.

Why: This could indicate identity theft.

How: Visit **annualcreditreport.com** to request your free report.

TIP: Be careful what you share online and check your privacy settings on social networking sites.

Why: Information you share online could give identity thieves clues to your accounts, shopping and banking practices, or security questions.

How: Check the settings section of your social media accounts.

TIP: Don't store sensitive information on your phone (like passwords, PINs, online banking User IDs and other usernames).

Why: Malicious or insecure applications could access or share your personal data with unauthorized sources. Some applications might leave your data exposed. For example, your notes app is likely not designed to store sensitive information. Additionally, if your phone is lost or stolen, it will be easier for this information to be compromised.

TIP: Get creative with the answers to security questions.

Why: It may be relatively easy for an identity thief to discover information such as your model of car or where you went to school.

How: Choose more unique questions or silly answers, which can confound the criminals while being memorable for you.

TIP: Consider installing an ad blocker on your browser.

Why: These can both save annoyance and help to protect you from malicious advertisements.

How: Be sure to research the ad browser before installing it on your computer, tablet, or smartphone.

TIP: Check gas pumps and ATMs for skimming devices.

Why: A card slot that feels a little bit tight can indicate the presence of a “skimmer,” which is one method thieves use to steal credit and debit card numbers.

How: Check for stickiness like adhesive residue, a card slot that sticks out a bit too far, anything hanging from the ATM, or anything that seems unusually loose about the card slot or keypad.